Table of Contents

Network......1

TCP Performance Tuning for WAN Transfers......1

Optional Advanced Tuning for Linux......3

NAS VPN Service......5

NAS Remote Network Diagnostic Tools......9

Increasing File Transfer Rates......10

Network

TCP Performance Tuning for WAN Transfers

DRAFT

This article is being reviewed for completeness and technical accuracy.

The purpose of this document is to help you maximize your wide-area network bulk data transfer performance by tuning the TCP settings for your end hosts. These are some common configuration tasks for enabling high performance data transfers on your system.

Making changes to your system should only be done by a lead system administrator or someone who is authorized to make changes.

Linux

1. Edit */etc/sysctl.conf* and add the following lines:

   ```
   net.core.wmem_max = 4194304
   net.core.rmem_max = 4194304
   ```

2. Then have them loaded by running "sysctl -p".

Windows

We recommend using a tool like Dr. TCP

Set the "Tcp Receive Window" to at least 4000000, turn on "Window Scaling", "Selective Acks", and "Time Stamping".

Other options for tuning Windows XP TCP are the SG TCP Optimizer or using Windows Registry Editor to edit the registry, but this is only recommended for Windows users who are already familiar with registry parameters.

Mac

- **Do these steps for OS 10.4**

These changes require root access.

In order to allow the Mac operating system to retain the parameters after a reboot, edit the following variables in */etc/sysctl.conf*:

```
# Set maximum TCP window sizes to 4 megabytes

net.inet.tcp.sendspace= 4194304
net.inet.tcp.recvspace= 4194304
# Set maximum Socket Buffer sizes to 4 megabytes

kern.ipc.maxsockbuf= 4194304
```

- **Do these steps for OS 10.5 and up**

  Use the **sysctl** command for the following variable:

  ```
  sysctl -w net.inet.tcp.win_scale_factor=8
  ```

If you follow these steps and are still getting less than your expected throughput, please contact the network group at support@nas.nasa.gov attn: Networks and we will work with you on tuning your system to optimize file transfers. You can also try the additional steps outlined in the following documents: Optional Advanced Tuning For Linux and Tips for File Transfers.

Optional Advanced Tuning for Linux

DRAFT

This article is being reviewed for completeness and technical accuracy.

This document describes additional TCP settings that can be tuned on high performance Linux systems. This is intended for 10 Gigabit hosts, but can also be applied to 1 Gigabit hosts. The following steps should be taken in addition to the steps outlined in TCP Performance Tuning for WAN transfers.

Configure the following */etc/sysctl.conf* settings for faster TCP:

Set maximum TCP window sizes to 12 megabytes

```
net.core.rmem_max = 11960320
net.core.wmem_max = 11960320
```

Set minimum, default, and maximum TCP buffer limits

```
net.ipv4.tcp_rmem = 4096 524288 11960320
net.ipv4.tcp_wmem = 4096 524288 11960320
```

Set maximum network input buffer queue length

```
net.core.netdev_max_backlog = 30000
```

Disable caching of TCP congestion state (Linux Kernel version 2.6 only). Fixes a bug in some Linux stacks.

```
net.ipv4.tcp_no_metrics_save = 1
```

Use the BIC TCP congestion control algorithm instead of the TCP Reno algorithm, Linux Kernel versions 2.6.8 to 2.6.18

```
net.ipv4.tcp_congestion_control = bic
```

Use the CUBIC TCP congestion control algorithm instead of the TCP Reno algorithm, Linux Kernel versions 2.6.18+

```
net.ipv4.tcp_congestion_control = cubic
```

Set the following to 1 (should default to 1 on most systems):

```
net.ipv4.tcp_window_scaling =1
net.ipv4.tcp_timestamps = 1
net.ipv4.tcp_sack = 1
```

A reboot will be needed for changes to */etc/sysctl.conf* to take effect, or you can attempt to reload sysctl settings (as root) with 'sysctl -p'.

For additional information visit this web site

If you have a 10Gig system or if you follow these steps and are still getting less than your expected throughput, please contact support@nas.nasa.gov attn: Networks and we will work with you on tuning your system to optimize file transfers.

NAS VPN Service

DRAFT

This article is being reviewed for completeness and technical accuracy.

For remote users wishing to connect to limited resources available on the local NAS network, a virtual private network service is available to any existing NAS user who has a Lou account and active SecurID fob. Additionally, NAS support staff may also make use of this service to provide some remote support to your government systems while on travel or at home.

*** ALL system traffic is routed through NAS while you are connected via VPN ***

This system is intended for government use and users are required to follow the appropriate use policy. All traffic is monitored. While connected, **ALL** your traffic will be routed through NAS, as if you were physically connected to NASLAN. When you are finished with your session, please remember to log out.

Users are subject to the NAS VPN Security Policy.

When and Why to use VPN:

The VPN service will make your system appear to be logically within the NAS external network, with some access to internal resources. Connection to the VPN server and installation of the VPN software are handled through Javascript and users do not have to pre-install prior to connection. VPN makes use of your standard web browser for encryption.

Through VPN, users can make use of any of the following services:

- Apple file sharing (AFP remote mount)
- Access to the NAS license server
- Access to the internal NAS webserver
- Access to some ARC websites not accessible from the outside
- SSH and SCP directly into NASLAN systems (NOT to Enclave systems)

How to Login to NAS VPN:

The login site is at: https://nas-vpn.nas.nasa.gov

Enter your login credentials (remember, it is your Lou account information and SecurID fob).

Click "Sign In", and you will be taken to the default VPN page upon successful authentication.

If it is the first time connecting from a new system, you will be prompted to install some software. Depending on your browser's security level, you may get a banner on top of the page warning you that the site is trying to install an ActiveX control. Click on that banner to install it.

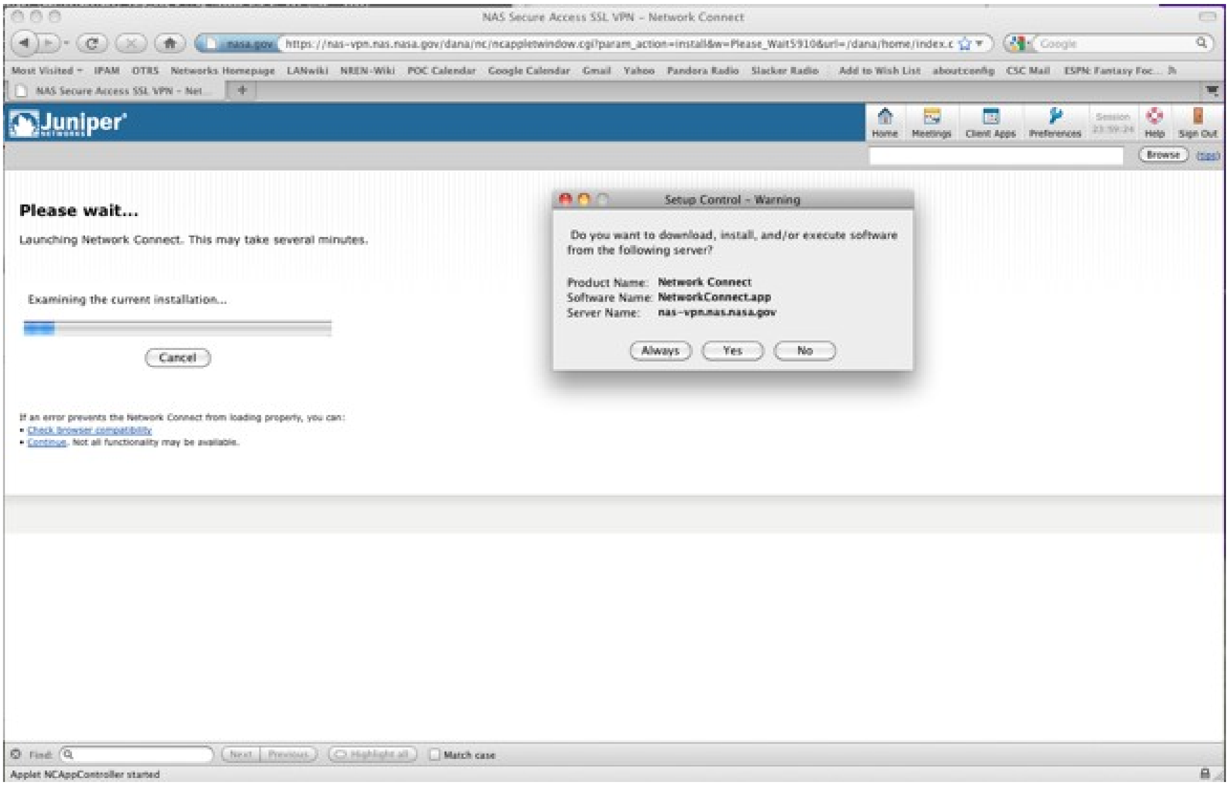
A pop-up window will show that the connection is negotiating. If it does not automatically start, click on "Start" under the Client Application Session for Network Connect. This may take up to a minute. Once done, the window will close and you will have been assigned a new IP address inside the VPN environment. A little icon will be placed in your desktop tray which you can use to get session information and disconnect.

You can verify that the VPN is working by connecting to:

http://myipaddress.com

Your address should be on the 198.9.30.x network.

NAS Supported systems already have the VPN Client installed on them. Just double click the "Network Connect" icon and enter your authentication credentials.



NAS Secure Access SSL VPN – Network Connect

https://nas-vpn.nas.nasa.gov/dana/nc/ncappletwindow.cgi?param_action=install&w=Please_Wait5910&url=/dana/home/index.c

Please wait...

Launching Network Connect. This may take several minutes.

Examining the current installation...

If an error prevents the Network Connect from loading properly, you can:
- Check browser compatibility
- Continue. Not all functionality may be available.

Setup Control – Warning

Do you want to download, install, and/or execute software from the following server?

Product Name: **Network Connect**
Software Name: **NetworkConnect.app**
Server Name: **nas-vpn.nas.nasa.gov**

Applet NCAppController started

Alternatively, if you cannot connect through the above methods, you can manually download the VPN client software here:

- Download VPN client for Mac
- Download VPN client for Linux
- Download the tar file which contains the VPN client for Windows
- Download the tar file which contains the VPN client for Windows 64 bit systems

VPN FAQ's:

- DO I need to keep my web browser open to keep the VPN up?

  No, you do not need to keep your web browser open once you start up the Network Connect client.
- How do I disconnect from the VPN?

  You can either go back to http://nas-vpn.nas.nasa.gov and click the "Sign Out" button on the top right corner, or right-click on the icon in your system tray and select "Sign Out".
- Is there an auto-logout?

  Yes. You will be logged out after 30 minutes of inactivity. The max session length is 12 hrs before you need to re-authenticate and you will be given a reminder before being disconnected. This is so that people don't stay "camped" on the VPN network.
- What traffic is sent over the VPN?

  ALL traffic you send will be sent over the VPN. This includes any websites you visit, any chat programs, or any software that requires a network connection. Because of this, it is important that you disconnect from the VPN while not in use.
- What changes are made to my system?

  Several changes are made to your network including a new IP address, default route, search domain and other minor files which allow you to be "virtually" inside the NASLAN. This means you can refer to hosts just by their hostname and not their fully-qualified name - eg:

  ssh username@desktop
- What browsers are supported?

  As long as you meet the requirements listed above, you should be able to connect on Safari, Internet Explorer, and Firefox. We recommend you update to the latest stable version. The minimum browser requirements are:

  - ♦ 168-bit and greater encryption
  - ♦ SSLv3 and TLSv1
  - ♦ JRE / Java enabled
  - ♦ Pop-up Windows

- How will connecting to the VPN impact my home network?

Some of your home services may stop working while connected to the VPN. This includes services like Internet printing, file sharing, and audio streaming. This is to ensure security of NAS while you are connected to the VPN.

NAS Remote Network Diagnostic Tools

A NAS network service that enables remote users to test end-to-end connectivity to the NAS HECC enclave is now available. Users can access the Network Diagnostic Tool service and initiate tests at: http://npad.nas.nasa.gov.

The diagnostic tests can only run on a Java-enabled web browser. If you have trouble accessing the website, please contact the NAS Control room (see below) and we will assist you.

Features

- Tools are accessible from any standard web browser
- Command-line tools are also available for Linux servers
- Users receive a diagnostic report on the test results; a copy of the report is sent to the NAS Networks team for analysis. If any problems are identified, the team will contact you to help resolve the issue.

The services available on this website run from inside the NAS network and are connected at 10 Gigabit Ethernet rates.

The Network Diagnostic Tester (NDT) - Performs a quick test that reports the maximum throughput to your remote system from NAS. It will also identify any issues with possible bad cabling, negotiation issues, packet loss, or general network congestion.

Network Path Application Diagnosis (NPAD) tool - Performs a more elaborate connection test and determines problems with TCP parameters, buffer sizes, and/or router congestion, and notifies you of recommended settings for maximum performance.

Traceroute tool - Allows users to perform reverse traceroutes from NAS display the path and measure transit delays of packets to a remote host.

Ping tool - Allows users to perform reverse pings from NAS to the remote host, to test the reachability to your host and measure round-trip time for messages to reach the remote host.

If you want a command line interface, you can also download client software and link to various other public services from this website.

If you have any questions about these new services, please contact the NAS Control Room staff 24x7 at (800) 331-8737, (650) 604-4444, support@nas.nasa.gov.

Increasing File Transfer Rates

One challenge users face is moving large amounts of data efficiently to/from NAS across the network. Often, minor system, software, or network configuration changes can increase network performance an order of magnitude or more. This article describes some methods for increasing data transfer performance.

If you are experiencing slow transfer rates, try these quick tips:

- Transfer using the bridge nodes (bridge1, bridge2) instead of the Pleiades front-end systems (PFEs). The bridge nodes have much more memory, along with 10-Gigabit Ethernet interfaces to accommodate many large transfers. The PFEs often become oversubscribed and cause slowness.
- If using the scp command, make sure you are using OpenSSH version 5 or later. Older versions of SSH have a hard limit on transfer rates and are not designed for WAN transfers. You can check your version of SSH by running the command ssh -V.
- For large files that are a gigabyte or larger, we recommend using BBFTP. This application allows for transferring simultaneous streams of data and doesn't have the overhead of encrypting all the data (authentication is still encrypted).

Online Network Testing Tools

The NAS PerfSONAR Service provides a custom website that that allows you to quickly self-diagnose your remote network connection issues, and reports the maximum bandwidth between sites, as well as any problems in the network path. Command-line tools are available if your system does not have a web browser.

Test results are also sent to our network experts, who will analyze traffic flows, identify problems, and work to resolve any bottlenecks that limit your network performance, whether the problem is at NAS or a remote site.

One-on-One Help

If you still require assistance in increasing your file transfer rates, please contact the NAS Control Room at support@nas.nasa.gov, and a network expert will work with you or your local administrator one-on-one to identify methods for increasing your rates.

To learn about other network-related support areas. see also, End-to-End Networking Services.